CANONICAL

Technical White Paper

Integrating Ubuntu 8.04 LTS into Microsoft Active Directory using Likewise Open

By Etienne Goyer – August 2009

www.canonical.com

Overview

Microsoft Active Directory is a widely-deployed directory service that is commonly used for identity management and authentication across the enterprise. Its ubiquity makes it a fixture of the IT landscape. As a result, interoperability with Active Directory is often a necessity when deploying services based on non-Microsoft operating systems.

Likewise Open, a tool whose purpose is precisely to ease integration of non-Microsoft operating systems into an existing Active Directory architecture, has been added to the Ubuntu base distribution starting with version 8.04 LTS. Likewise Open automates a set of settings that previously required time-consuming and error-prone manual configurations, making integration of Ubuntu with Active Directory quick and painless as it takes the guesswork out of the process. Likewise Open also supports disconnected operations, bringing network directory access to laptop users. This white paper will demonstrate how Likewise Open can ease Ubuntu deployment in an Active Directory-based infrastructure whether on the desktop or the server..

It is important to understand that Active Directory was never been meant to be a cross-platform directory service in the first place. From the ground up, it was built with Microsoft operating systems and software in mind, with little thought given to third-party products. As such, complete Active Directory integration of third-party operating systems, such as Ubuntu, is hardly possible. The identity management component of Active Directory (authentication of users and groups) is open enough for tools such as Likewise Open to achieve a functional level of interoperability. However, do not assume further Active Directory tasks, such as system management and provisioning for example, are interoperable with Ubuntu.

Fortunately, innovative software solutions exist to fill in the functionality gap. One such tool is Likewise Enterprise, of which Likewise Open is a subset. Likewise Enterprise provides a set of tools to enable the use of group policies with Linux (including Ubuntu) and Mac OS desktops, along with seamless integration into Active Directory-native management tools. If such a feature would be beneficial to you, you are encouraged to ask Likewise Software (info@likewisesoftware.com) directly, or discuss your specific needs with your Canonical sales executive for further recommendations.

Table of Contents

Introduction

This white paper discusses the use of Likewise Open on Ubuntu 8.04 LTS. Firstly, we will demonstrate how an Ubuntu desktop can be configured to enable Active Directory users to login. Later in the paper, we will provide an example of how an Ubuntu server can be configured to resolve and authenticate users of a network service against Active Directory. Both of these tasks will be achieved using Likewise Open.

Content

The section 'Overview of Likewise Open' explains what Likewise is, and briefly presents its architecture with an eye toward understanding how it fulfills its functions in Ubuntu.

Pre-requisites and configuration checklists for both Active Directory and Ubuntu members are discussed in the 'Active Directory setup checklist' and 'Ubuntu setup checklist', respectively. This section is not specific to our example setup; it holds true for any deployment of Likewise Open, and can be used as a starting point of your own.

The section 'Integrating Ubuntu with Active Directory' presents the steps required to connect an Ubuntu Server Edition server from the command line, or an Ubuntu Desktop Edition machine using the Likewise-provided graphical applet. At the end of this section, you will be able to log in to your Ubuntu machines using Active Directory credentials.

'Ubuntu network service authentication to Active Directory through Active Directory' discusses an example application where centralised authentication is put to good use. In the example provided , a mail server running IMAP authenticates its user to the Active Directory with the help of Likewise Open.

Finally, we present a number of alternatives to Likewise Open and discuss their advantages and drawbacks.

Intended audience

This white paper has been written with Windows system administrators new to Ubuntu in mind. We assume a basic level of knowledge of administering Ubuntu, including the ability to use a command-line shell, understanding of sudo as a means for privilege escalation and the ability to use a text editor to edit configuration files.

Meet Warthogs LLC

Throughout this white paper, we will use a fictional corporation called Warthogs LLC. Warthogs LLC is a fine provider of African sophism with a booming world-wide market. Warthogs employs three people in its Montréal office in Canada: Alice, Bob and Carol. Coincidentally, all three share an unexplained fascination for cryptography. Alice acts as the system administrator for the office, and as the CEO of the company; she is a long-time Ubuntu user. Bob, the salesman, also takes care of various clerical duties and prefers the use of Windows XP on his desktop. Carol, the marketing webmaster, uses Ubuntu on her desktop as a powerful and versatile development platform. Alice manages both the Active Directory controller (ADC) and an Ubuntu file and web server. Alice, after investigating tools to ease the integration of Ubuntu into her Active Directory infrastructure, settled on Likewise Open.

The Montréal branch office network is currently equipped with four computers:

Computer name	Operating system	IP address	Role
adc1.warthogs.biz	Windows Server 2008	192.168.4.221	Domain controller
ubuntusrv1.warthogs.biz	Ubuntu 8.04 LTS Server Edition	192.168.4.222	File server
xpdesktop1.warthogs.biz	Windows XP Professional	192.168.4.223	Office workstation
ubuntudesktop.warthogs.biz	Ubuntu 8.04 LTS Desktop Edition	192.168.4.224	Web development workstation

The Active Directory domain is warthogs.biz. For the sake of simplicity, the directory is comprised of a single domain and a single site within the forest, and that domain is not subdivided into organisational units.

Overview of Likewise Open

The information in this white paper is based on Likewise Open version 4.0.5, as shipped in Ubuntu 8.04 LTS, and believed to be correct for that version. As is typical with most Open Source projects, Likewise Open is under heavy development so new versions are released on a regular basis. These new versions are likely to introduce fixes and improvements for issues discussed in this document.

The purpose of Likewise Open is to simplify integration of Linux and Mac OS into Microsoft Active Directory. It is based in some part on a component of the Samba open source project called winbind. The purpose of winbind is to act as a gateway to Microsoft domains for authentication and identity resolution of users, and to provide consistent mapping of users and groups. It basically enables Microsoft domain users and groups to appear to be local on the non-Microsoft system. This is very useful in a number of scenarios, particularly when sharing files between Windows and Linux using Samba.

To make full use of winbind as a source of local users and groups on Linux requires a fair bit of effort. The Name Service Switch (NSS) framework needs to be configured to resolve users and groups against winbind. The Pluggable Authentication Module (PAM) stack similarly needs to be configured to funnel authentication requests through winbind. The behaviour of winbind itself is configurable to a large extent, and getting the intended result may involve tweaking its configuration considerably. Likewise Open consolidates all these operations in a single tool and delivers a clean configuration for the common use-case in a few easy steps.

Likewise Open, through a PAM module, provides a generic mechanism for system services on Ubuntu to validate user's credentials against Active Directory. This would allow, for example, a mail server, a web service, or any other application that supports the PAM framework, to authenticate users belonging to the Active Directory the Ubuntu server is joined to. This pre-empts the need to keep multiple redundant authentication databases by centralising user accounts management, and enables organisations to make full use of their existing Active Directory infrastructures and know-how when deploying Ubuntu.

Once Likewise Open is installed and configured, users from the Active Directory will appear as if they are local to the Ubuntu system. User attributes that are standard in Unix/Linux but not present in Active Directory are either generated algorithmically on the fly (ie, the numerical user id), or through configuration directive (home directory location and preferred user shell.) In the same manner, groups from the Active Directory will also appear to be regular Unix groups. This is achieved through a Name Service Switch (NSS) module, a mechanism that is standard across all Linux distributions.

Likewise Open provides both a graphical applet and a command-line tool which share a common backend. The graphical applet is available from the menu, as System > Administration > Likewise. It makes joining an Active Directory very straightforward. The command-line tool, domainjoin-cli, does the same and a little more, such as various sanity checks on the Ubuntu computer's configuration (more on that later). A set of command-line utilities (lwimsg, lwiinfo and lwinet) is also provided for advanced troubleshooting and configuration.

Under the hood, Likewise Open is running a daemon (a long-running system service) called likewise-winbindd. Its job it is to arbitrate communication to the Active Directory Controller (ADC) on behalf of the PAM and NSS modules discussed above. The likewise-winbindd daemon also takes care of caching credentials and user's information, allowing disconnected operation; this is useful for laptop users, and as a resiliency measure against network and ADC failures.

Advantages of Likewise Open

- No software to install on the Active Directory, and no change to its configuration required.
- Centralised authentication use existing user and group when deploying Ubuntu, no need to maintain duplicate user database.
- Unix user and group id are coherent across all machines running Likewise Open, no need to maintain an id map.
- Disconnected operation enables mobile users to authenticate using their Active Directory credentials.

Drawbacks

- No control over assignment of Unix user and group id; they are computed algorithmically by Likewise Open.
- No fine-grained control over which Active Directory users and groups are exposed by Likewise Open client.
- Integration limited to identity management and authentication (but see the sub-section on Likewise Enterprise at the end of this white paper for information on a more feature-full alternative.)

Active Directory setup checklist

Here is a quick checklist of things to have or to verify before we jump in and start using Likewise Open.

DNS

Before you can join a Ubuntu machine to an Active Directory, you will need to ensure that a DNS entry has been created for the machine in question.

> Please note that, starting with Ubuntu 8.10, users no longer need to manually creating a DNS record to connect the Ubuntu host to the domain using Likewise Open; the record is created and updated automatically.

While not strictly a requirement, it is better to have a reverse lookup zone configured (containing pointer (PTR) records) for your domain in the Active Directory DNS, as many services in Linux do make use of reverse lookup. From the Ubuntu command line, you can easily check if the reverse lookups have been configured properly by using the dig or the host command:

```
ubuntu@ubuntusrv1:~$ host 192.168.4.224
224.4.168.192.in-addr.arpa domain name pointer
ubuntudesktop1.warthogs.biz.
ubuntu@ubuntusrv1:~$ dig -x 192.168.4.223

; <<>> DiG 9.4.2 <<>> -x 192.168.4.223
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10566
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;223.4.168.192.in-addr.arpa.    IN      PTR

;; ANSWER SECTION:
223.4.168.192.in-addr.arpa. 1200 IN     PTR     xpdesktop1.warthogs.biz.

;; Query time: 1 msec
;; SERVER: 192.168.4.221#53(192.168.4.221)
;; WHEN: Wed Jan 28 14:33:39 2009
;; MSG SIZE  rcvd: 81
```

Organisational Unit

If your Active Directory domain is divided into organisational units (OU), you will need to determine into which OUs you want to join the Ubuntu computers. In this white paper, we will not make use of OUs.

Administrative privileges

You will need an account with sufficient privileges to add the Ubuntu computers to the Active Directory. Typically, this would be an account member of the Domain Administrator group (such as the ubiquitous Administrator account), although this can vary according to your Active Directory configuration.

Ubuntu setup checklist

Here is a brief list of things to verify before you can use Likewise Open to connect an Ubuntu machine to an Active Directory.

Network settings

Using Likewise Open obviously requires network connectivity to the ADC. While it is possible to use Likewise Open on a machine configured for dynamic IP addressing using DHCP, our example will assume fixed IP settings with a single network interface for the sake of simplicity.

If a firewall is mitigating IP connectivity between the Ubuntu machine and the ADC, you will need to ensure that the required ports are open for connection between the ADC and the Ubuntu machines. Please refer to the 'Likewise Open Installation and Administration Guide' (see the “Further reading” section at the end of this document) for the complete list of ports required. Likewise Open itself is not listening on any port for an inbound connection; as such, no change will need to be made if you are using a host-based firewall, such as iptables or ufw, on the Ubuntu machine.

Host name

It is important to ensure that the fully qualified domain name (FQDN) of the Ubuntu machine matches the DNS record used in the Active Directory DNS. This information is stored in the /etc/hostname configuration file on Ubuntu, and a matching entry must exist in /etc/hosts. You can check the FQDN of the Ubuntu machine from the command line using the “hostname” command, for example:

```
ubuntu@ubuntusrv1:~$ hostname -f
ubuntusrv1.warthogs.biz
```

Likewise Open provides a way to quickly fix the FQDN on Ubuntu machines without directly editing the configuration file, using the domainjoin-cli command with the setname and fixfqdn argument, for example:

```
ubuntu@ubuntusrv2:~$ sudo domainjoin-cli setname ubuntusrv1
ubuntu@ubuntusrv2:~$ sudo domainjoin-cli fixfqdn
```

You can then verify again that the host name is correct using the “hostname -f” command, as above. Rebooting is not necessary for the change to be applied.

Time synchronisation

The Kerberos protocol, used internally by Active Directory for authentication, is sensitive to clock skew between computers participating in a Kerberos domain. The default clock skew tolerance is 300 seconds (five minutes). If the Ubuntu machine and the ADC clock drift apart for more than five minutes, authentication against the ADC will systematically fail.

Traditionally, in the Unix/Linux world, time synchronisation is achieved using the Network Time Protocol (NTP). This is usually completed against an external time source, such as one of the many public NTP servers on the Internet. By default, Ubuntu is configured to synchronise time with the ntp.ubuntu.com NTP server each time a network interface is brought up, which happens at least at every boot.

In our case, it is not desirable to have the Ubuntu machine synchronise time with an outside source, as this source may differ from the ADC. Hence, the default NTP server needs to be changed to one of the ADC. This is done by changing the value of the NTPSERVERS variable in /etc/default/ntpdate. In our case, we need to use /etc/default/ntpdate, which appears as below:

```
# The settings in this file are used by the program ntpdate-debian, but
not
# by the upstream program ntpdate.

# Set to "yes" to take the server list from /etc/ntp.conf, from package
ntp,
# so you only have to keep it in one place.
NTPDATE_USE_NTP_CONF=yes

# List of NTP servers to use  (Separate multiple servers with spaces.)
# Not used if NTPDATE_USE_NTP_CONF is yes.
NTPSERVERS="adc1.warthogs.biz"

# Additional options to pass to ntpdate
NTPOPTIONS=""
```

You can manually synchronise time by invoking the ntpdate-debian command as the super user, for example:

```
ubuntu@ubuntusrv1:~$ sudo ntpdate-debian
28 Jan 20:19:50 ntpdate[4358]: step time server 192.168.4.221 offset
-1.457341 sec
```

On long-running Ubuntu servers, where time is not synchronised frequently through a reboot, you may want to use a cron job to invoke the ntpdate-debian command periodically.

Administrative privileges

As is usual in Ubuntu, all examples of command requiring super-user (administrative) privileges in the text have been prefixed with sudo. You are not expected to have access to the root account (it is disabled by default on Ubuntu), but you are expected to have a user account member of the admin group, who is allowed to escalate privileges using the sudo command. The first user account, created during installation, is a member of the admin group in question. In our case, this user is called, quite simply, 'ubuntu'.

Connecting Ubuntu to the Active Directory

Once all the conditions discussed in the checklist sections above are met, you are ready to proceed with connecting Ubuntu computers to your Active Directory.

Using the command line

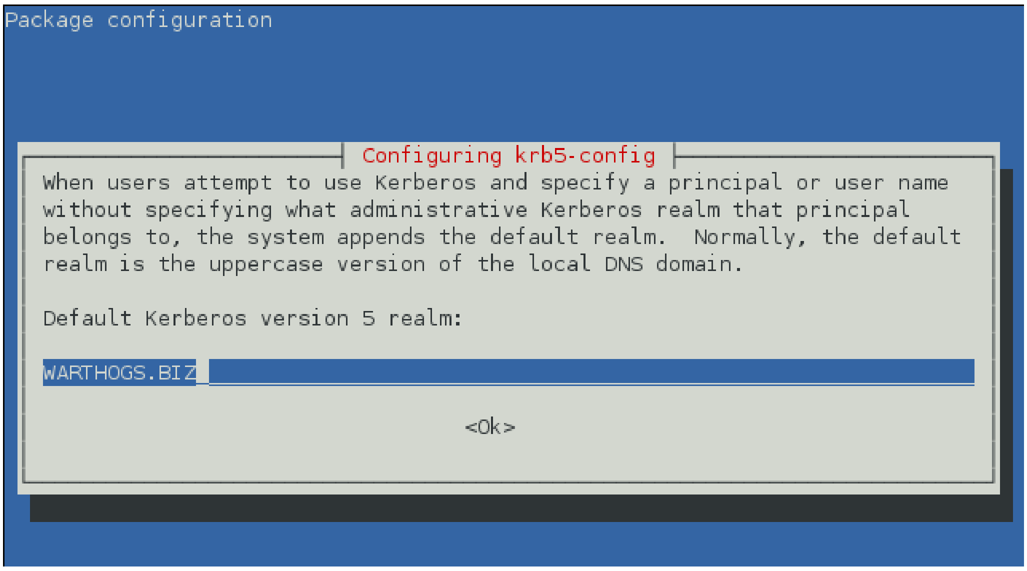
On an installation of Ubuntu Server Edition, you would use the domainjoin-cli command-line tool as super-user to proceed.

Installing Likewise Open

The first step is to install the likewise-open package from the Ubuntu online software repository using apt-get, as it is not installed by default.

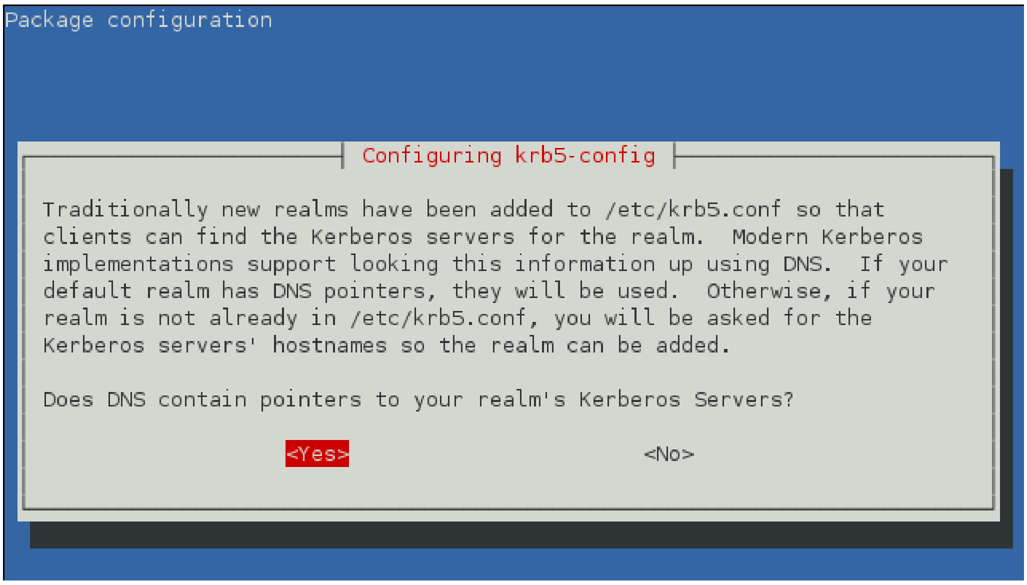
```
ubuntu@ubuntusrv1:~$ sudo apt-get install likewise-open
```

During the package installation, you will be prompted to configure Kerberos. The base Kerberos libraries are required, as they are invoked by Likewise Open. You will need to provide information relevant to your Active Directory.



```
Package configuration

                 ┤ Configuring krb5-config ├
 When users attempt to use Kerberos and specify a principal or user name
 without specifying what administrative Kerberos realm that principal
 belongs to, the system appends the default realm.  Normally, the default
 realm is the uppercase version of the local DNS domain.

 Default Kerberos version 5 realm:

 WARTHOGS.BIZ_

                                <Ok>
```

When prompted for your Kerberos realm, provide your Active Directory domain name. By convention, Kerberos realms name are all capitalised, although this is not a strict requirement.



```
Package configuration

              ┤ Configuring krb5-config ├

 Traditionally new realms have been added to /etc/krb5.conf so that
 clients can find the Kerberos servers for the realm.  Modern Kerberos
 implementations support looking this information up using DNS.  If your
 default realm has DNS pointers, they will be used.  Otherwise, if your
 realm is not already in /etc/krb5.conf, you will be asked for the
 Kerberos servers' hostnames so the realm can be added.

 Does DNS contain pointers to your realm's Kerberos Servers?

                <Yes>                              <No>
```

As Active Directory actually does provide DNS pointers to your realm's Kerberos servers (ie, the ADC), you can safely answer 'Yes' to this question. This will greatly simplify the Kerberos configuration.

Joining the domain

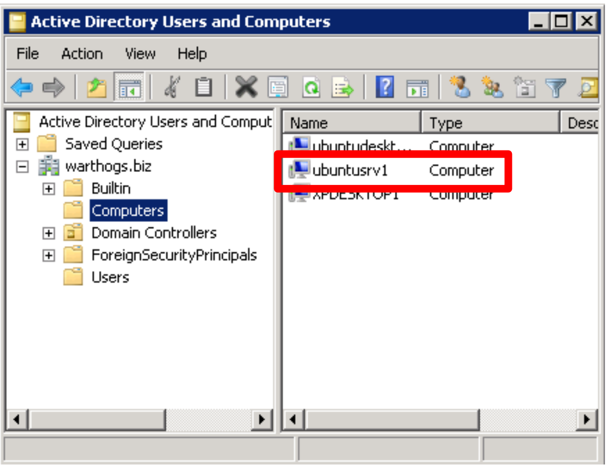
Once the likewise-open package is installed, you can proceed with joining the domain using the domainjoin-cli command-line tool, for example:

```
ubuntu@ubuntusrv1:~$ sudo domainjoin-cli join warthogs.biz Administrator
Joining to AD Domain:   warthogs.biz
With Computer DNS Name: ubuntusrv1.warthogs.biz

Administrator@WARTHOGS.BIZ's password: *****
SUCCESS
```

You can substitute 'warthogs.biz' for your own domain name, and 'Administrator' for an account with sufficient privileges to join computers in your domain. And that's it!

Verifying proper domain operations

To verify that Likewise Open works as intended, you may want to check that the Ubuntu server is listed in the Active Directory Users and Computers MMC snap-in.



On the Ubuntu computer, confirm that it has indeed joined the domain by querying Likewise Open, for example:

```
ubuntu@ubuntusrv1:~$ sudo domainjoin-cli query
Name = ubuntusrv1
Domain = WARTHOGS.BIZ
Distinguished Name = CN=ubuntusrv1,CN=Computers,DC=warthogs,DC=biz
```

Next, verify that users from the domain can be resolved using the getent command, for example:

```
ubuntu@ubuntusrv1:~$ getent passwd WARTHOGS\\alice
WARTHOGS\alice:*:878183504:878182913:Alice
Rivest:/home/WARTHOGS/alice:/bin/bash
```

The getent command is used to query NSS databases. In the above case, we ask getent to query the passwd database for the 'WARTHOGS\alice' entry. The entry format is the same as is used in the /etc/passwd system user database, except the entry is not actually from /etc/passwd; it is pulled from the Active Directory. You may also use getent to resolve a group entry, as below:

```
ubuntu@ubuntusrv1:~$ getent group WARTHOGS\\marketing
WARTHOGS\marketing:x:878183507:WARTHOGS\bob,WARTHOGS\carol
```

Notice that both users and groups from the Active Directory are prefixed with the domain name according to the usual DOMAIN\ convention.

The backslashes "\" have a special meaning as the so-called "escape" character in Unix shells. As such, when you use the DOMAIN\user convention at a shell prompt, the backslash will need to be doubled to prevent escaping, for example DOMAIN\\user. Alternatively, you can quote the expression containing a backslash, as with 'DOMAIN\user'.

Lastly, you can test authentication by using SSH to connect to your Ubuntu server. As we already have a shell running on the Ubuntu server, we can simply open an SSH connection to 'localhost' using an Active Directory user, for example:

```
ubuntu@ubuntusrv1:~$ ssh –l WARTHOGS\\alice localhost
Password:
Last login: Fri Jan 30 15:41:33 2009 from localhost
WARTHOGS\alice@ubuntusrv1:~$ whoami
WARTHOGS\alice
WARTHOGS\alice@ubuntusrv1:~$ id
uid=878183504(WARTHOGS\alice) gid=878182913(WARTHOGS\domain^users)
groups=878182913(WARTHOGS\domain^users),878183508(WARTHOGS\engineering)
```

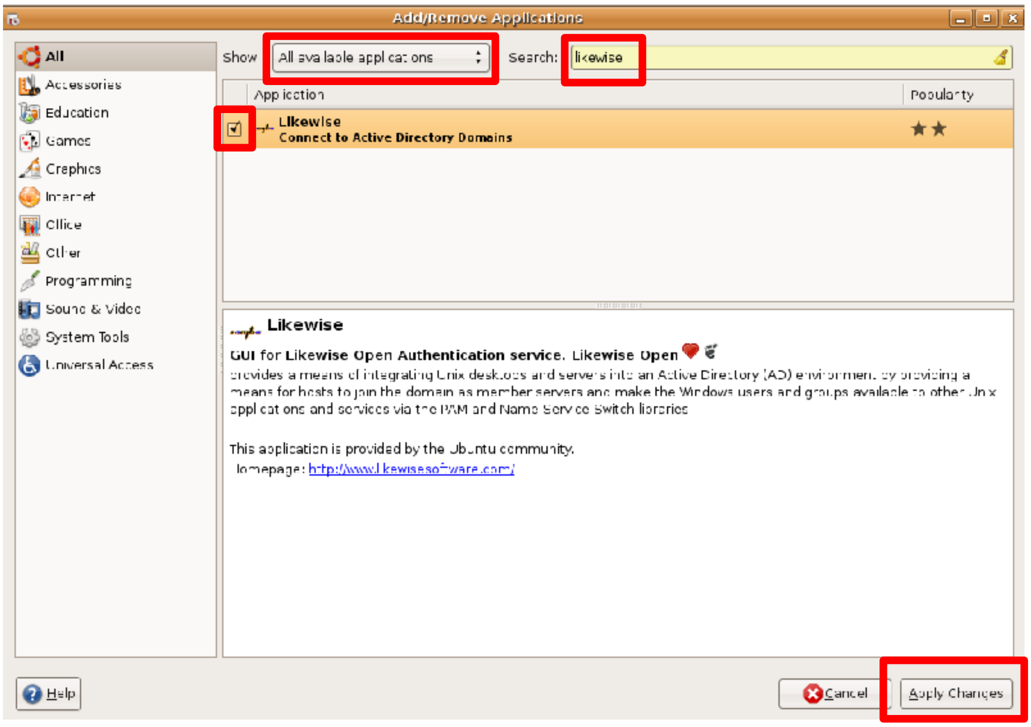
From the above, we can see that we were able to establish an SSH connection using the credentials of an Active Directory user, confirming the ability to authenticate to the Active Directory. The 'whoami' and 'id' commands further confirm that resolving users and groups work as expected. We have finished testing the installation.

Using the graphical Likewise AD Settings applet

The command-line procedure described above would work on either Ubuntu Server Edition or Ubuntu Desktop Edition. However, with Ubuntu Desktop, you can also use the graphical Likewise AD Settings applet.

Installing Likewise Open

The graphical applet is installable via the 'likewise-open' package. You can install it using your choice of software package management tool. The easiest way is by using the Add/Remove Applications applet (Applications > Add/Remove...)



Likewise

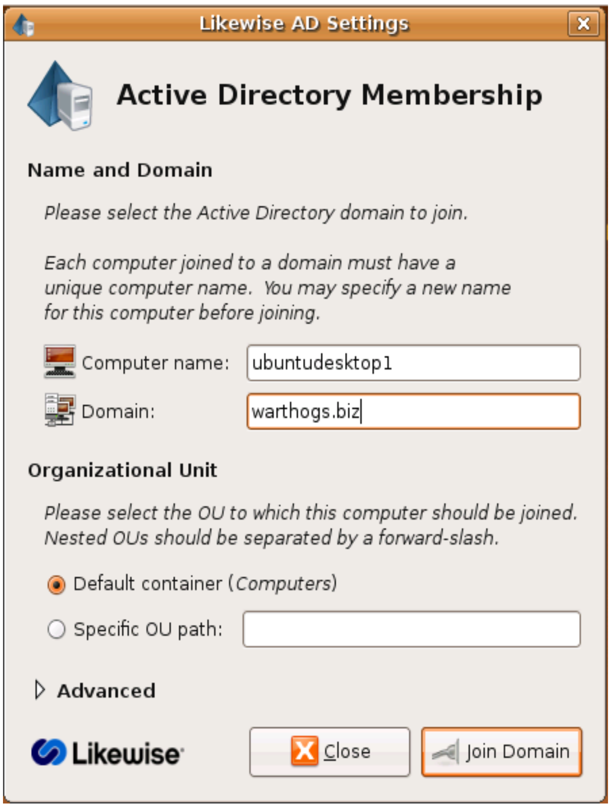
GUI for Likewise Open Authentication service. Likewise Open provides a means of integrating Unix desktops and servers into an Active Directory (AD) environment by providing a means for hosts to join the domain as member servers and make the Windows users and groups available to other Unix applications and services via the PAM and Name Service Switch libraries

This application is provided by the Ubuntu community.
Homepage: http://www.likewisesoftware.com/

When installing Likewise Open from the Add/Remove Applications applet, you may be prompted to 'enable the community-maintained software repository'. Likewise Open itself is part of the main Ubuntu software repository, and as such is supported and maintained by Canonical. However, the graphical applet provided by Likewise Open to join a domain is part of the community-maintained software repository (also called 'universe'). There is no harm in enabling the community-maintained software repository for the purpose of installing the Likewise Open graphical component. But if you would rather make sure that only software maintained and supported by Canonical is installed from there on, you will need to disable the community-maintained online software repository in System > Administration > Software Sources.

Joining the domain

You can start Likewise AD Settings from System > Administration > Likewise. The applet is self-explanatory; you will need to provide the computer name and the domain name to join.



Active Directory Membership

Name and Domain

Please select the Active Directory domain to join.

Each computer joined to a domain must have a unique computer name. You may specify a new name for this computer before joining.

Computer name: ubuntudesktop1

Domain: warthogs.biz

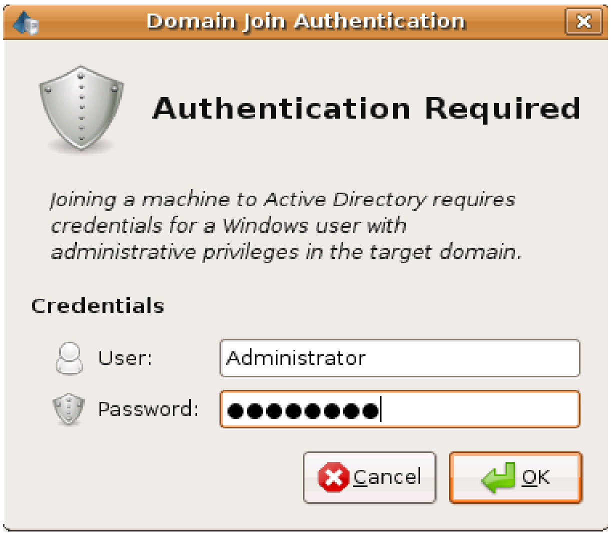
Organizational Unit

Please select the OU to which this computer should be joined. Nested OUs should be separated by a forward-slash.

● Default container (*Computers*)

○ Specific OU path:

You will also need to provide credentials of a user authorised to connect computers to the domain.



Authentication Required

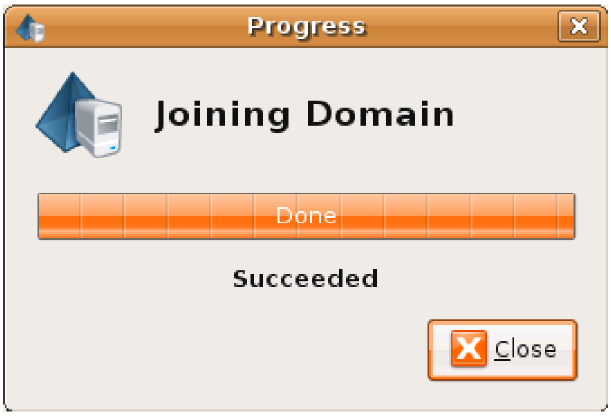
Joining a machine to Active Directory requires credentials for a Windows user with administrative privileges in the target domain.

Credentials

User: Administrator

Password: ●●●●●●●●

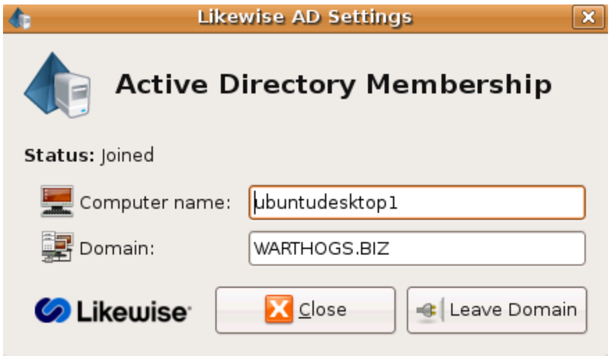
After a short while, you will be presented with a confirmation that the computer has successfully joined the domain.



Succeeded

Verifying proper domain operation

You can then review the settings by invoking the Likewise AD Settings applet again from System > Administration > Likewise.



Status: Joined

Computer name: ubuntudesktop1

Domain: WARTHOGS.BIZ

You may go through the command-line verification explained earlier if you wish. A good test is to simply log into GNOME using an Active Directory account (do not forget to prefix the username with DOMAIN\, like “WARTHOGS\alice”).

Once Likewise Open has been installed and you have confirmed that it works as expected, you are ready to start using Ubuntu as a member of your Active Directory.

Ubuntu network services authentication to Active Directory through Likewise Open

In this section, we will see how a network service hosted on Ubuntu can be configured to resolve and authenticate users against an Active Directory, using the existing enterprise directory.

We will use IMAP to demonstrate this capability, specifically using the Dovecot mail server. IMAP is a popular standard for accessing mailboxes from a Mail User Agent (MUA), such as Mozilla Thunderbird, GNOME Evolution or Microsoft Outlook. Dovecot is the default Mail Delivery Agent (MDA) in Ubuntu. It is a light-weight, secure, standard-compliant MDA that is easy to configure and supports the IMAP and POP3 protocols. Dovecot will use the Likewise Open Pluggable Authentication Module (PAM) and Name Service Switch (NSS) library. Users connecting to the IMAP service will provide their credentials at the prompt, and Dovecot will validate them using Likewise Open.

We are using Dovecot to illustrate the capabilities brought in by using Likewise Open to join an Active Directory, but we could have used just about any server software that uses the standard NSS and PAM mechanisms, such as SSH or FTP.

Installing and configuring Dovecot IMAP server

> For the purpose of this white paper, we will reduce the configuration of Dovecot to the bare minimum required to illustrate how to make it authenticate users to an Active Directory using Likewise Open. Hence, various topics such as SSL or mailbox formats are out of scope and will not be discussed. Moreover, in the real world, you would need a Mail Transfer Agent (MTA) such as Postfix to receive emails and deliver them to Dovecot, which we will not discuss here.

The Dovecot IMAP server is installable from the Ubuntu online software repository. It can be installed in a single command using apt-get, as below:

```
sudo apt-get install dovecot-imapd
```

Once installed, modifications will need to be done to its configuration file, /etc/dovecot/dovecot.conf. This file is abundantly commented and provides a good starting point for a complete configuration. By default, very little change is required as Dovecot authenticates using PAM and resolves user and group information using NSS already. The only change we need to make is to add the '\' character to the list of allowed characters in username (in bold below.)

```
protocols = imap imaps
log_timestamp = "%Y-%m-%d %H:%M:%S "
mail_privileged_group = mail

disable_plaintext_auth = no
auth_username_chars =
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ01234567890.-_@\
auth default {
  mechanisms = plain
  user = root
  passdb pam {
  }
  userdb passwd {
  }
}
```

The above minimal dovecot.conf example leaves out the comments and empty configuration directives for clarity.

Please note that the 'disable_plaintext_auth = no' directive above is considered insecure, as it implies that Dovecot will accept passwords sent in clear text over the network. Do not use this directive in a real-world installation; configure IMAPS (IMAP over SSL) instead.

Once you have made the required changes, you can restart the Dovecot service with the following command:

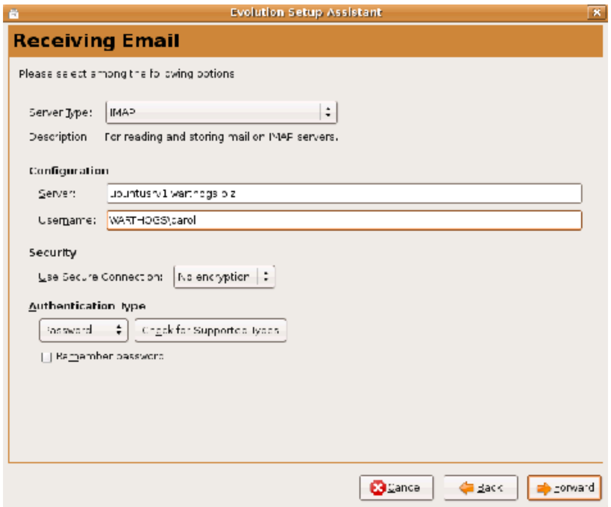
```
sudo /etc/init.d/dovecot restart
```

You can then test the connection from a client machine.

Configuring Ubuntu 8.04 LTS as a client

Evolution is the default Mail User Agent (MUA) in Ubuntu, and is installed by default as Applications > Internet > Evolution Mail. Many other MUAs are available for installation from the Ubuntu online software repository, such as Mozilla Thunderbird or Kmail. We will stick to Evolution for the purposes of this example.

The first time you start Evolution, the Evolution Setup Assistant will be run. You will be prompted for identity information, whether or not you want to restore the account details from a backup, and for the incoming server details. In our case, we will use the following configuration:


Evolution Setup Assistant

Receiving Email

Please select among the following options

Server Type: IMAP

Description: For reading and storing mail on IMAP servers.

Configuration

Server: ubuntusrv1.warthogs.biz

Username: WARTHOGS\carol

Security

Use Secure Connection: No encryption

Authentication Type

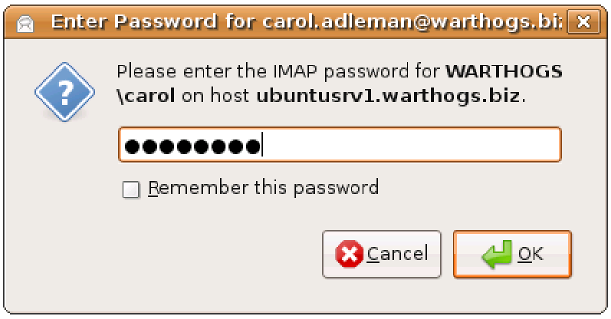
Password

□ Remember password

It is important to use the DOMAIN\user convention when specifying the username, as this is how Likewise Open exposes the Active Directory users to the Ubuntu system, including the Dovecot server.

From there on, you can provide appropriate information in the subsequent dialog boxes to complete the assistant.

Once finished with the assistant, you will be prompted to provide your mail account password. This will be the Active Directory password for the user in question.

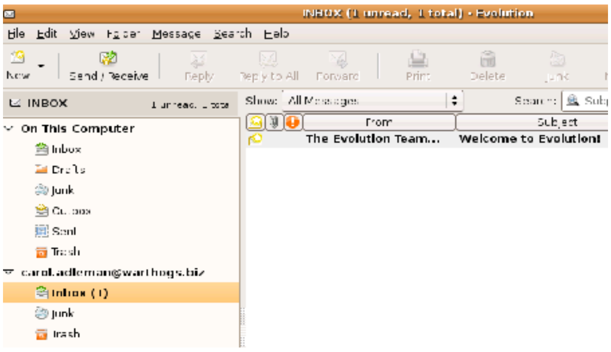

Enter Password for carol.adleman@warthogs.bi:

Please enter the IMAP password for **WARTHOGS\carol** on host **ubuntusrv1.warthogs.biz**.

●●●●●●●●

□ Remember this password

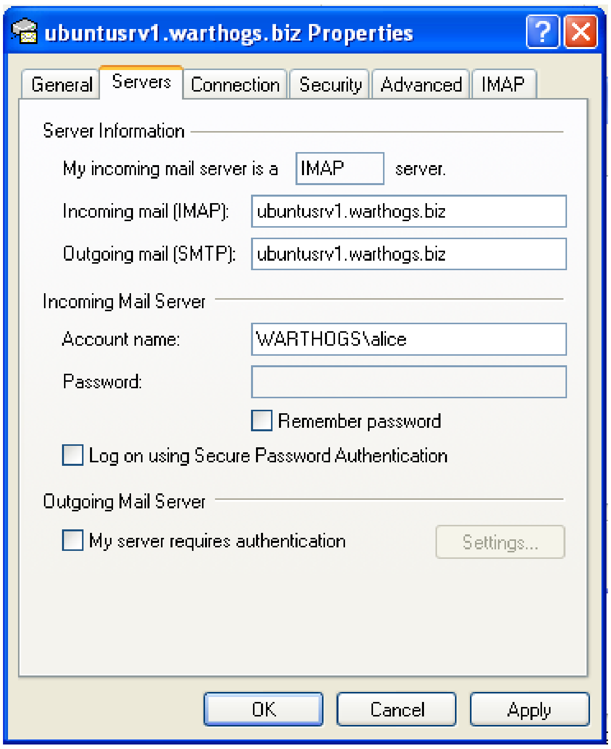
You will be able to see your IMAP inbox once you are logged in.



Configuring Windows XP as a client

Here, we demonstrate how Outlook Express can be configured to retrieve email from our IMAP server, using Active Directory user credentials, in the same manner as Evolution was configured in the previous section.

Configuration is similar to that of Evolution. We use 'ubuntusrv1.warthogs.biz' as the incoming mail server name, and 'WARTHOGS\alice' as the username.



Server Information

My incoming mail server is a IMAP server.

Incoming mail (IMAP): ubuntusrv1.warthogs.biz

Outgoing mail (SMTP): ubuntusrv1.warthogs.biz

Incoming Mail Server

Account name: WARTHOGS\alice

Password:

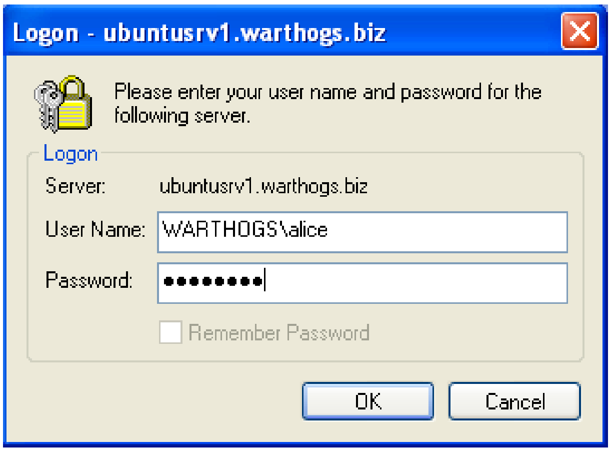
□ Remember password

□ Log on using Secure Password Authentication

Outgoing Mail Server

□ My server requires authentication

Once the account has been created, you can log in to the mail server.



Logon - ubuntusrv1.warthogs.biz

Please enter your user name and password for the following server.

Logon

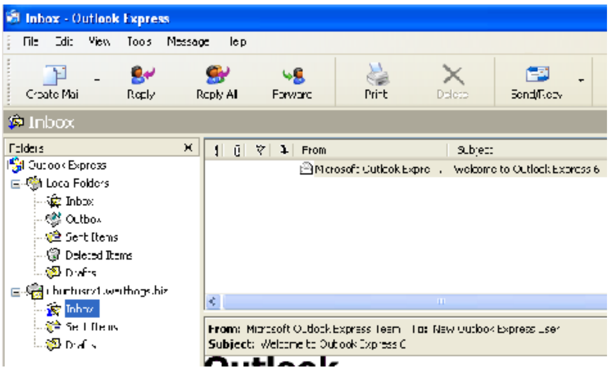
Server: ubuntusrv1.warthogs.biz

User Name: WARTHOGS\alice

Password: ●●●●●●●●●

□ Remember Password

You will be able to see your IMAP inbox once you are logged in.



Inbox - Outlook Express

From: Microsoft Outlook Express Team To: New Outlook Express User
Subject: Welcome to Outlook Express 6

Alternative to Likewise Open

If, for some reason, Likewise Open is not suitable for your environment, there are other options that can help you integrate Ubuntu into Active Directory for authentication and identity management.

Likewise Enterprise

Likewise Software, the company behind Likewise Open, also offers an enterprise version of its interoperability software. Likewise Enterprise offers a range of features useful in a large-scale deployment and a Group Policy for use with supported platforms such as Ubuntu. It also includes an ADC management console, integration with the Active Directory Users and Computers MMC snap-in, extended auditing and reporting features, an NIS migration assistant, SSO capabilities for Apache and Samba, and much, much more.

You can learn more about Likewise Enterprise at
http://www.likewise.com/products/likewise_enterprise/index.php

NSS and PAM configured for LDAP and Kerberos

Microsoft Active Directory is based, in part, on the LDAP and Kerberos standards. Both of these protocols are well supported in the Linux world. LDAP can be used as a database for NSS, and both LDAP and Kerberos can be used as an authentication backend with PAM. Combined together, you can get the same result as using Likewise Open, without the disconnected operations.

Unix user and group accounts requires a certain number of attributes that are not present by default in Active Directory. Starting with Windows Server 2003 R2, the Active Directory schema have been extended to include attributes conforming to RFC 2307 - “An Approach for Using LDAP as a Network Information Service”, which defines the LDAP attributes required by Unix and Unix-like system, such as Ubuntu. A role service, Identity Management for UNIX, is available in Active Directory to extend functionalities precisely for that purpose. From there on, Active Directory can be used as a store of Unix users and groups as is, without the help of third-party tools. This approach may prove more flexible than using Likewise Open, at the cost of being more management-heavy.

On the Ubuntu side, a set of configurations for the components involved will need to be documented and deployed. Starting with release 7.10, Ubuntu ship with a template-based framework for configuring NSS and PAM called auth-client-config, which could be used to ease the process.

On the Active Directory side, RFC2307 attributes of users and groups will need to be set and managed. While installing the Identity Management for UNIX role service extend the Active Directory Users and Computers MMC snap-in to expose these attributes and allows for setting their value manually, a large deployment will certainly need some sort of tool to automate the process. This needs to be taken into consideration.

Plain winbind

As explained in the “Overview of Likewise Open” section, Likewise Open is based on winbind, a part of the Samba open source project. Winbind itself includes PAM and NSS modules to authenticate and resolve users and groups to an Active Directory. It is generally used alongside Samba for file sharing services, where it exposes Windows domain users as local Unix users.

Its use, however, is not restricted to Samba: it would also work well with any services that use NSS and PAM for user management. For example, our demonstration involving Dovecot would work just as well with a properly configured winbind installation. This would involve modifying /etc/nsswitch.conf (the system NSS configuration file) and /etc/pam.d/ (the PAM system configuration directory) to use winbind.

One of winbind's tasks is to keep a mapping of Unix numerical user and group id for Windows user and groups. By default, winbind assigns Unix uid and gid sequentially as users and groups are being looked up. The result is, obviously, rather random and will vary from one machine running winbind to another. This will pose a problem if your infrastructure requires Unix and Unix-like machines to share a coherent uid and gid namespace; that would be the case if, for example, you where to share files using the Unix-native NFS protocol. Fortunately, winbind can be configured to use a so-called idmap backend that can be shared among multiple winbind instances. The job of these idmap backends is to store the Windows SID to Unix id mapping, ensuring that users and groups id are consistent across all machines using the same backend. For example, such an idmap could ensure that the Active Directory user WARTHOGS\alice has a user id 13897 on both server ubuntusrv1 and ubuntusrv2, making file permissions manageable and consistent when files are being shared between the two. Various idmap backend are available, and winbind can also be configured to derive Unix id algorithmically based on the Windows RID, just like Likewise Open.

If you wish to learn more about winbind, the best reference remains the Offical Samba HOWTO and Reference Guide at

http://samba.org/samba/docs/man/Samba-HOWTO-Collection/

Further reading

Likewise Open Installation and Administration Guide

- For version 4.1, but largely applicable to 4.0.5 too.

http://www.likewise.com/resources/user_documentation/Likewise-Open-Guide.pdf

The Ubuntu Server Guide

- A good starting point for everything Ubuntu-related, including sections on LDAP, Kerberos and even Likewise Open!

http://doc.ubuntu.com/ubuntu/serverguide/C/

IETF RFC 2307 - An Approach for Using LDAP as a Network Information Service

- For directory administrator interested in knowing the exact purpose of all LDAP attributes used by NSS.

http://www.ietf.org/rfc/rfc2307.txt

Kerberos Explained

- A dated but excellent article on Microsoft's implementation of the Kerberos protocol. Despite the source, the explanations are surprisingly platform-agnostic.

http://technet.microsoft.com/en-us/library/bb742516.aspx

Every effort has been made by Canonical to ensure the accuracy of this document but Canonical disclaims, to the extent possible at law, any liability for any error or omission.

Any information contained in this document may change without notice and Canonical is not held responsible for any such changes.